CLAIMS

1. A method for securely distributing a cryptographic key, said method comprising the steps of:

combining the cryptographic key with a transport key to form a key set;

encrypting the key set to form an encrypted key set;

distributing the encrypted key set across a medium; and

decrypting the encrypted key set to reconstitute the cryptographic key and the transport key.

2. The method of claim 1 wherein:

the combining, encrypting, and distributing steps are performed by a first party; and

the decrypting step is performed by a second party in preparation for entering into secure communications with the first party.

3. The method of claim 1 wherein the medium comprises an electronic network.

4. The method of claim 1 wherein the medium comprises an insecure network.

5. The method of claim 1 wherein the medium comprises the Internet.

6. The method of claim 1 further comprising the step of, prior to the combining step, compressing the transport key to form a compressed transport key.

7. The method of claim 6 wherein the volume of the compressed transport key is no more than 50% of the volume of the transport key before it is compressed.

8. The method of claim 6 wherein the compressing step is performed by a method of key folding, so that the volume of the compressed transport key is 50% of the volume of the transport key before it is compressed.

9. The method of claim 6 wherein the compressing step is performed using at least one process from the following:

advanced matrix arithmetic compression;

vector based compression;

quantum compression;

sliding window compression;

key folding using bit swapping.

10. The method of claim 6 wherein:

the compressing step is performed by a method of key folding using bit swapping;

most significant bits of each byte in the transport key are discarded; and

bit positions created by said discarded most significant bits in a given byte are filled with least significant bits from another byte of the transport key.

11. The method of claim 6 wherein:

the decrypting step yields the cryptographic key and the compressed transport key; and

said method further comprises the step of:

after the decrypting step, decompressing the compressed transport key to reconstitute the transport key.

12. The method of claim 1 wherein the cryptographic key is adapted for use in a One-Time Pad cipher system.

13. The method of claim 12 wherein the encrypting step is performed using an exclusive OR operation.

14. The method of claim 1 wherein the encrypting step and the decrypting step are performed using the same key.

15. The method of claim 1 wherein the cryptographic key is a private key adapted for use in a public key cryptosystem.

16. The method of claim 1 wherein the cryptographic key is a symmetric key adapted for use in a symmetric key cryptosystem.

17. The method of claim 1 wherein:

the steps of combining, encrypting, distributing, and decrypting are repeated a plurality of iterations; and

the transport key from a given iteration is used as the key that performs the encrypting step and the decrypting step in a subsequent iteration.

18. The method of claim 17 wherein the repetition of the combining, encrypting, distributing, and decrypting steps is terminated after a preselected event has occurred.

19. The method of claim 17 wherein the combining step is initiated by an imminent expiration of a cryptographic key that was distributed in a previous iteration.

20. The method of claim 1 wherein the encrypting step is performed by a key comprising a transport key from a previous iteration of the method XORed with a conversion key.

21. The method of claim 20 wherein the conversion key is a subset of the cryptographic key.

22. The method of claim 20 wherein the conversion key is generated by a true random number generator.

23. The method of claim 20 wherein the method is performed a plurality of iterations, and a new conversion key is generated during each iteration.

24. A computer-readable medium containing computer program instructions for securely distributing a cryptographic key, said computer program instructions performing the steps of:

combining the cryptographic key with a transport key to form a key set;

encrypting the key set to form an encrypted key set;

distributing the encrypted key set across a medium; and

decrypting the encrypted key set to reconstitute the cryptographic key and the transport key.

25. Apparatus for securely distributing a cryptographic key from a first party to a second party, said apparatus comprising:

means for generating the cryptographic key;

means for generating a transport key;

means for encrypting the cryptographic key and the transport key to form an encrypted key set;

means for distributing the encrypted key set across a medium; and

means for decrypting the encrypted key set to reconstitute the cryptographic key and the transport key.